OIPE
MAY 21 2001
PATENT & TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of		Saqib Jang et al.	Date	:	May 18, 2001
Serial No.	:	09/819,548			
Filing Date	:	March 26, 2001	Our Docket	:	MGC 302
For	:	MULTIPLE SUBSCRIBER VIDEOCONFERENCING SYSTEM			

Commissioner of Patents
Washington, D.C. 20231

Sir:

PRELIMINARY AMENDMENT

Preliminary to the review of the above identified application, please enter the following amendments. As required by 37 C.F.R. § 1.121, applicants have provided a separate marked-up version of the amended claims showing the changes relative to the previous version of those claims (attached). Please enter the following amendments preliminary to the examination of the above identified application.

In the Specification:

Please replace paragraph 2 on page 1 with the following.

--Technical Field

The present invention relates generally to videoconferencing, and more particularly to a system, method, and device for implementing a multiple subscriber videoconferencing service for use on Internet Protocol (IP) networks.--

05/23/2001 SDENBOB1 00000010 09819548
01 FC:202 150.00 OP
02 FC:203 360.00 OP

Please replace paragraph 2 on page 2 with the following.

--Videoconferencing over IP networks has a number of fundamental problems, including security, bandwidth utilization, quality of service, and deployment and management. Regarding security, H.323 and SIP are difficult to implement with current firewalls. The difficulty lies in the fact that H.323 and SIP are complex protocols and use multiple dynamically allocated ports for each call. Because of the heavy use of dynamically allocated ports, it is not possible to preconfigure firewalls to allow SIP- or H.323-signaled traffic without opening up large numbers of holes in the firewall. This represents a more lax firewall policy than would be acceptable at most enterprises. In addition, SIP or H.323 video endpoints behind a firewall typically cannot receive calls from external parties due to firewall policies in place at most enterprises.--

Please replace paragraph 1 on page 4 with the following.

--The above discussed issues lead to another problem with current videoconferencing systems, namely, that enterprises cannot easily outsource videoconferencing services to outside service providers. Currently, service providers are not able to cost-effectively provide videoconferencing services to a large number of subscribers, because specialized equipment must be deployed or existing equipment must be upgraded at every subscriber site. This results in an expensive up-front capital investment as well as significant operational expenses for the service provider. Up-front equipment installations take time at each subscriber, resulting in a slow deployment of the

videoconferencing capabilities to subscribers. In addition, the high up-front costs result in decreased service provider profit margins. It is difficult to grow such a service because each subscriber adds to an incremental growth in the capital equipment pool because these resources are not shared.--

Please replace paragraph 2 on page 4 with the following.

--Because of the cost and reliability issues with ISDN, and because of the security, bandwidth utilization, quality of service, and deployment and management issues with H.323 and SIP, it is difficult for the average enterprise to upgrade and customize its network to enable videoconferencing. In addition, it is difficult for service providers to cost-effectively provide an outsourced videoconferencing service on a per-subscriber basis. Thus there exists a need for a videoconferencing system, method, and device for delivering secure, high-quality videoconferencing services over an IP network to multiple enterprise subscribers in a manner that does not require expensive upgrading and customization of the enterprise network.--

Please replace paragraph 2 on page 5 with the following.

--According to another embodiment of the invention, the method may include installing a video services switch on a service provider network at an access point configured to enable multiple enterprise subscribers to access a global packet-switched computer network to exchange data, including videoconferencing data and non-

videoconferencing data. The video services switch is typically configured to process videoconferencing data from multiple enterprise subscribers. The method further includes, at the video services switch, receiving a request for a videoconferencing call from an origination endpoint of one of the multiple enterprise subscribers, and connecting the videoconferencing call to a destination endpoint, the videoconferencing call having associated videoconferencing data. The method may further include securing the videoconferencing call based on subscriber-specific security settings.--

Please replace paragraph 2 on page 6 with the following.

--The system typically includes a service provider network configured to enable users of multiple enterprise subscriber networks to transfer data via a global computer network, the service provider network having an access point. The system also includes a videoconferencing services switch located on the access point of the service provider network. The videoconferencing services switch is configured to process videoconferencing calls from terminals on each of the multiple subscriber networks, based on subscriber-specific settings.--

Please replace paragraph 6 on page 6 with the following.

--Fig. 4A is a software architecture of the videoconferencing system of Fig. 1.

Fig. 4B is a continuation of the software architecture of Fig. 4A.--

Please replace paragraph 4 on page 7 with the following.

--Fig. 9 is a flowchart of one exemplary method for accomplishing the step of configuring the user-specific and subscriber-specific settings of the method of Fig. 6.--

Please replace paragraph 3 on pages 8-9 with the following.

--Traffic coming into the POP can be classified into videoconferencing data and non-videoconferencing data. Videoconferencing data typically includes control data and streaming voice and audio data according to the H.323 or SIP standards. H.323 refers to International Telecommunications Union, Telecommunications Sector, Recommendation H.323 (version 1, published November 1996; version 2, published 1998, entitled, "Visual Telephone Systems and Equipment for Local Area Networks Which Provide a Non-guaranteed Quality of Service," the disclosures of which are herein incorporated herein by reference. SIP refers to Session Initiation Protocol Proposed Standard (RFC 2543), Internet Engineering Task Force (IETF) (published March 1999), the disclosure of which is incorporated herein by reference. Non-videoconferencing data includes, for example, email, web pages, VOIP traffic, VPN traffic, etc. Videoconferencing data is typically routed through POP 16 via videoconferencing services switch 12, while non-videoconferencing data is routed around the switch.--

Please replace paragraph 2 on page 9 with the following.

--Each of enterprise subscriber networks 18 typically includes a plurality of terminals 34. Terminals 34, along with video conferencing service switch 12 and the various other components of system 10, are typically H.323 or SIP compliant. Terminals 34 are typically videoconferencing devices configured to display and record both video and audio. Terminals 34 may be desktop computers, laptop computers, mainframes and/or workstation computers, or other videoconferencing devices. Terminals 34 may also be described as "endpoints" in a videoconferencing call. The terminal 34a originating the videoconferencing call is referred to as an origination endpoint 34a, and the other terminals requested to join in the call are referred to as destination terminals, shown at 34b, 134a, 134b. Terminal 34b is a local zone destination terminal, while terminals 134a, 134b are remote zone destination terminals. Local and remote zones are defined below.--

Please replace paragraph 4 on pages 9-10 with the following.

--Enterprise video gateway 36 typically includes an emulation module 40 which emulates H.323/SIP call control and firewall functionality and an encryption module 44. The gateway also typically has a globally routable IP address and is configured to manage secure communication between terminals 34 and the videoconferencing services switch 12. Typically, emulation module 40 appears to terminals 34 as H.323 gatekeeper/SIP proxy and H.323/SIP application proxy firewall

which includes network address translation (NAT) capability, which hides internal address from outside devices.--

Please replace paragraph 2 on page 10 with the following.

--As shown in Fig. 10, enterprise video gateway 36 includes an encryption module 44. Encryption module 44 is typically an IP Security (IPSec) authentication and encryption module 44 configured to encrypt videoconferencing data coming from terminals 34 and send the encrypted data to videoconferencing switch 12. The IPSec protocols have been adopted by the Internet Engineering Task Force, and are described in the RFC 2411 entitled "IP Security Document Roadmap" (published Nov. 1998), the disclosure of which is herein incorporated by reference. By using IPSec, a Virtual Private Network (VPN) may be created between the gateway 36 and the switch 12. VPN refers to a network that is carried over public networks, but which is encrypted to make it secure from outside access and interference.--

Please replace paragraph 3 on page 11 with the following.

--System 10 may be configured to connect a two-party or multiparty videoconference call from an origination terminal 34a to a destination terminal 34b on local zone 11, and/or one or more destination terminals 134a and 134b on remote zone 111. A destination terminal on local zone 11 may be referred to as a local destination

terminal, and a destination terminal on remote zone 111 may be referred to as a remote destination terminal.--

Please replace paragraph 5 on pages 11-12 with the following.

--Each enterprise subscriber network 218 includes a plurality of terminals 234 which are similar to terminals 34 described above. Integrated Access Device (IAD) 246 is configured to receive traffic from enterprise subscriber networks 218 and forward the traffic to the Digital Subscriber Line Access Multiplexor (DSLAM) 248. The DSLAM is configured to multiplex the traffic from the IADs and forward it to Asynchronous Transmission Mode (ATM) switch 250, where the signals are demultiplexed for transmission over a long-haul backbone. ATM switch 250 is configured to route videoconferencing data to and from terminals 234 and the backbone via videoconferencing services switch 212, and non-videoconferencing data via ISP router 252, or another services switch.--

Please replace paragraph 2 on page 12 with the following.

--Fig. 3 shows an exemplary hardware configuration for videoconferencing services switch 12. One switch that may be purchased and programmed to implement the present invention is the Intel Exchange Architecture (IXA) WAN/Access switch, commercially available from Intel Corporation, of Santa Clara, California and Radisys Corporation of Hillsboro, Oregon.--

Please replace paragraph 3 on pages 12-13 with the following.

--Switch 12 typically includes a control plane module 302 and a data plane module 304. Control plane module 302 includes a host processor, linked to an input/output network interface 308 and a memory 310. Typically, memory 310 includes RAM and ROM, although another form of memory may also be used, such as flash memory. Alternatively, a storage device such as a hard drive may also be attached to host processor 306. Control plane module 302 is configured to receive control data such as call set-up information through network interface 308, data plane ingress port 318, or data plane egress port 320. The call set-up information is processed according to H.323 or SIP specifications by host processor 306. Typically, the programs and data necessary for processing the call are stored in memory 310 and implemented by host processor 306. For example, the virtual router, call control module, quality of service module, policy engine, and security module are typically stored in memory 310.--

Please replace paragraph 3 on pages 12-13 with the following.

--Control plane module 302 is linked to data plane module 304 via a bus 312. Data plane module 304 includes a network processor 314 and memory configured to receive and manage transfer of real-time audio and video data streams from ingress ports 318 to egress ports 320. Data plane module 304 typically includes a wire-speed switching fabric, capable of processing real-time data streams with virtually no appreciable latency.--

Please replace paragraph 3 on page 13 with the following.

--The wire-speed switching fabric is configured to enable transport of streaming data traffic across system with virtually no appreciable latency, even as the streaming data traffic is processed and analyzed by system 10 to impose H.323/NAT-specific firewall and NAT capabilities, policies from policy engine 418, monitor quality of service, and provide optional encryption and other security measures. One implementation of system 10 is configured to provide aggregate streaming data throughput of up to 1.048 Gbps with full security and policy management, quality of service management, and encryption. The wire-speed switching fabric includes full support for IETF standard IP routing protocols such as Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), and Routing Information Protocol (RIP), which are well known in the networking arts. Support of these routing protocols will allow system 10 to forward video traffic appropriately to edge router 20 and core router 22 in the service provider access point 116.--

Please replace paragraph 2 on page 14 with the following.

--Terminal settings 408a typically include the IP address of the enterprise gateway, which acts as a proxy to the call control module 413 in videoconferencing switch 12. For calls placed with the H.323 protocol, the IP address of the enterprise gateway 36 (which also acts as a proxy to the videoconferencing services switch H.323

gatekeeper 414) is provided. For calls placed with the SIP protocol, the IP address of the enterprise gateway 36 (which also acts as a proxy to the videoconferencing services switch SIP proxy 416) is provided. Terminals use the IP address of the enterprise gateway for registration (using e.g. H.323 RAS signaling), call initiation (using e.g. H.323 ARQ signaling), and audio/video data exchange (using e.g. RTP/RTCP protocols). Users may optionally authenticate themselves with H.323 gatekeeper/SIP proxy. The enterprise gateway 36 encapsulates these messages in packets having the enterprise video gateway's globally routable IP address as the source address and forwards these messages to the call control module 413 in videoconferencing services switch 12. Typically, these packets are sent in an encrypted form using IPSec.--

Please replace paragraph 2 on page 15 with the following.

--Enterprise edge router settings 408b typically include the globally routable IP address of the enterprise gateway 36, and the address of an H.323 gatekeeper 414 and/or SIP proxy 416 within the videoconferencing services switch 12. The enterprise edge router may also be configured to direct traffic from a terminal to the gatekeeper 414 or proxy 416 along direct connection 42. Enterprise edge router settings 408b may also include prioritization information for traffic passing though the edge router, such that the router may tag packets passing through with Diff-Serv labels or process packets based on Diff-Serv labels.--

Please replace paragraph 3 on page 16 with the following.

--Calls in the H.323 protocol are routed to virtual H.323 gatekeeper 414, while calls in the SIP protocol are routed to SIP Proxy 416. Call control module 413 is configured to perform call set-up operations, manage call data streams, and perform call tear-down operations.--

Please replace paragraph 3 on page 18 with the following.

--Quality of service module 420 also includes an IP-over-ATM module 428 configured to send IP traffic over ATM switches, and settings 408k therefor. IP over ATM module is compliant with the standards described in Internet Engineering Task Force Request for Comments (RFC) 2684. Typically, settings 408k for IP-over-ATM module 428 are configured on a per-virtual router and per-physical interface basis.--

Please replace paragraph 5 on pages 18-19 with the following.

--Videoconferencing services switch 12 also typically includes a security module 431. Security module 431 typically includes a SIP/H.323 firewall 432, SIP/H.323 NAT module 434, encryption module 436, and Virtual Private Network (VPN) module 438. SIP/H.323 firewall 432 is configured to prevent unauthorized access to video services switch 402, and through it to subscriber networks. The firewall settings 408n of firewall 432 are configured on a per-subscriber basis, such that a subscriber-specific firewall may be custom-implemented for traffic from each subscriber. SIP/H.323 NAT

module 434 is configured to provide network address translation services for traffic flowing through switch 12. NAT settings 408l are also subscriber-specific. VPN module 438 is configured to create a virtual private network for data flowing from switch 12 over network 20.--

Please replace paragraph 3 on pages 19-20 with the following.

--Videoconferencing services management application 402 is configured to interface with a database 404, which contains a database image 406 of records for subscriber-specific settings 408 for each of the multiple enterprise subscriber networks 18. Many of the subscriber-specific settings 408 are governed by a Service Level Agreement (SLA) 409. The SLA is an agreement executed between each enterprise subscriber and the service provider. The SLA contains terms for the level of videoconferencing service to be provided to a particular enterprise subscriber network. One exemplary term contained in the SLA is a video quality term, which indicates the maximum and/or minimum video quality the subscriber is to receive, either on a per-subscriber, per-user, or per-terminal basis. Often, video quality is defined as packet loss, jitter, and latency being within an acceptable predetermined range. While, typically, terminal settings 408a and enterprise router settings 408b are stored locally on enterprise subscriber network 18, it will also be appreciated that they may be stored on database 404. The switch resident settings are typically loaded into video services switch 12 periodically, such as once per day, by downloading database image 404 into memory of

switch 12. The enterprise video gateway server settings 408r may be downloaded in a similar manner from database 404 via videoconferencing services management application 402.--

Please replace paragraph 2 on page 23 with the following.

--Step 510 includes, at 612, configuring a call-control module. At 614, step 612 includes configuring H.323 gatekeeper 414 and/or SIP proxy 416 for subscriber 18. For H.323 gatekeeper 414, configuring gatekeeper 414 includes configuring a subscriber zone in gatekeeper 414, discovery and registration of endpoints, security, inter-gatekeeper communication, creation of records for billing and administrative purposes, etc. For SIP proxy 416, configuring proxy 416 includes discovery and registration of endpoints, information from Domain Name Service (DNS) server, creation of records, etc.--

Please replace paragraph 2 on page 24 with the following.

--Step 616 further includes configuring the encryption module at 706. Encryption is used only at certain enterprise subscribers 18 and destination IP addresses. For example, enterprises 18 may want encrypted communication with selected destination parties.--

Please replace paragraph 3 on page 24 with the following.

--Lastly, step 616 includes configuring virtual private network (VPN) module at 708. Configuring VPN module includes configuring a subscriber VR with MPLS VPN capability including creation of VPN routing/forwarding tables. Step 708 further includes configuring BGP routing sessions, VR to SP edge-routing sessions, RIP/BGP/static route to subscriber edge-routing sessions, etc. By configuring switch 12 to support an MPLS VPN module, video-specific VPNs can exist across ATM, IP and L2-type backbone networks. In addition, subscribers to MPLS VPNs may be dynamically updated to enable simplified creation of extranet and intranet VPNs and site-to-site video traffic delivery.--

Please replace paragraph 3 on page 25 with the following.

--At 806, the method further includes configuring differentiated services (Diff-Serv) module 426 at 806, typically by adjusting Diff Serv settings 408j. These settings may be used to configure the TOS/IP precedence field for video traffic (i.e. RTP streams) to/from each enterprise. This enables core devices in an SP network to give prioritized treatment to video traffic.--

Please replace paragraph 5 on page 25 with the following.

--At 810, the method further includes configuring video transmission analysis module, typically by adjusting settings 408m. Configuration of size of jitter buffer within the videoconferencing services switch is accomplished on a per-enterprise subscriber basis.--

Please replace paragraph 6 on pages 25-26 with the following.

--Fig. 9 shows, in steps 902-918, one exemplary method of accomplishing step 620 of configuring user-specific and subscriber-specific policies on policy engine 418. The method typically includes, at 902, setting access privileges. Access privileges govern who can access the video system with user level and administrator level access privileges. At 904, the method includes setting inbound/outbound calling privileges on a per-user or per-subscriber basis. For example, every user in an enterprise may be prohibited from making outbound calls on company holidays, except upper management. At 906, the method typically includes setting time-of-day privileges per user or subscriber. For example, every user may be restricted from placing calls outside of regular business hours. At 908, the method typically includes setting maximum video quality privileges per user, or per subscriber.--

Please replace paragraph 2 on page 26 with the following.

--At 910, the method typically includes setting 2-way support privileges.

This allows a user to either send, receive, or both send and receive videoconferencing data pertaining to a call. At 912, the method includes setting audio-only restrictions on a per-user or per-subscriber basis. The method includes setting encryption requirements at 914. At 916, the method typically includes setting priority privileges on a per-user or per-subscriber basis. Videoconferencing data sent by a user with higher priority privilege will take precedence over other data sent by a user of lower priority, or over other lower priority data, such as email. At 918, the method typically includes setting videoconferencing call screening. This enables a user or subscriber to block incoming calls from a user-specified source. The policies set in step 620, and substeps 902-918 are typically saved as user-specific and subscriber-wide settings 408f, 408g.--

09819548 052204

In the Claims:

Please cancel claims 18-20, without prejudice.

Please replace claims 1, 5-8, and 10 with the following amended claims 1, 5-8, and 10.

1. (Amended) A method for videoconferencing using Internet Protocol (IP), the method comprising the steps of:

installing a videoconferencing services switch at an access point to a service provider IP network;

at the switch, registering a plurality of subscribers for videoconferencing

services, each subscriber including a plurality of endpoints;

receiving subscriber-specific settings to be applied to multiple videoconferencing calls from the plurality of endpoints associated with each subscriber;

storing the subscriber-specific settings at a location accessible to the switch; and

configuring the switch to connect calls from the plurality of endpoints at each subscriber based on the corresponding subscriber-specific settings.

5. (Amended) A method for use in videoconferencing, the method comprising:

installing a videoconferencing services switch on a service provider network at an access point configured to enable multiple enterprise subscribers to access a global packet-switched computer network to exchange data, including videoconferencing data and non-videoconferencing data, the videoconferencing services switch being configured to process videoconferencing data from multiple enterprise subscribers;

at the videoconferencing services switch, receiving a request for a videoconferencing call from an origination endpoint of one of the multiple enterprise subscribers;

connecting the videoconferencing call to a destination endpoint, the videoconferencing call having associated videoconferencing data; and

securing the videoconferencing call based on subscriber-specific security settings.

6. (Amended) The method of claim 5, wherein each enterprise subscriber includes an enterprise gateway positioned on the network between the access point and the origination endpoint, the method further comprising:

routing videoconferencing data from the enterprise gateway to videoconferencing services switch; and

routing non-videoconferencing data from the enterprise gateway around the videoconferencing services switch.

7. (Amended) The method of claim 6, wherein the videoconferencing data is routed to the videoconferencing services switch via a direct network connection from an enterprise router to the videoconferencing services switch.

8. (Amended) The method of claim 6, wherein the videoconferencing data is routed to the videoconferencing services service switch through an access point edge router.

10. (Amended) The method of claim 9, wherein the videoconferencing data routed through the firewall is encrypted.

Please add new claims 21-61, as follows.

--21. A videoconferencing services switch, comprising:

a control plane module configured to receive subscriber-specific videoconferencing call settings for each of a plurality of enterprise subscribers, the videoconferencing call settings being for multiple calls placed from each enterprise subscriber;

a data plane module configured to receive videoconferencing data streams from the plurality of enterprise subscribers and manage these videoconferencing data streams according to the subscriber-specific videoconferencing call settings for each enterprise subscriber.

22. A videoconferencing services switch configured to process a videoconferencing call between an origination terminal and a destination terminal, the origination and destination terminals being located on one or more enterprise subscriber networks, the videoconferencing services switch comprising:

a virtual router configured to receive a request for a videoconferencing call from the origination terminal; and

a call control module configured to manage call data streams for the videoconferencing call, wherein the virtual router is configured to route call-related traffic between the originating terminal and call control module.

23. The videoconferencing services switch of claim 22, wherein the virtual router has a unique IP address for each of the enterprise subscriber networks.

24. The videoconferencing services switch of claim 23, wherein the virtual router includes subscriber-specific settings, and the virtual router is configured to route call-related traffic to/from the call control module based on the subscriber-specific settings.

25. The videoconferencing services switch of claim 24, wherein the subscriber-specific settings for the virtual router are selected from the group consisting of an address of an enterprise edge router, an address of an Integrated Access Device (IAD), information about a dedicated physical connection between the enterprise subscriber network and the videoconferencing services switch, and information on a POP edge router.

26. The videoconferencing services switch of claim 22, wherein the virtual router is configured to provide Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF) routing on a per-virtual router basis.

27. The videoconferencing services switch of claim 22, wherein the virtual router is configured to maintain separate routing tables for each subscriber to segment its traffic.

28. The videoconferencing services switch of claim 22, further comprising, a quality of service module having subscriber-specific settings for the quality of service of videoconferencing calls placed via the switch.

29. The videoconferencing services switch of claim 28, wherein the subscriber specific settings include bandwidth settings, and the quality of service module is configured to guarantee quality of service according to the subscriber-specific bandwidth settings.

30. The videoconferencing services switch of claim 28, wherein the quality of service module includes a Multi Protocol Label Switching (MPLS) traffic engineering module configured to create a network path for the videoconferencing call.

31. The videoconferencing services switch of claim 30, wherein the MPLS traffic engineering module is configured to create secure MPLS tunnels that offer a guaranteed bandwidth for videoconferencing traffic, based on subscriber-specific settings.

32. The videoconferencing services switch of claim 28, wherein the quality of service module includes a bandwidth management module configured to manage the bandwidth allocated to each videoconferencing call and/or terminal, based on subscriber-specific settings.

33. The videoconferencing services switch of claim 28, wherein the quality of service module includes a differentiated services module configured to implement differentiated services policy management.

34. The videoconferencing services switch of claim 33, wherein the quality of service module is configured to label a precedence parameter for videoconferencing traffic, based on a subscriber-specific setting.

35. The videoconferencing services switch of claim 28, wherein the quality of service module includes an IP over ATM module configured to send IP traffic over ATM switches, based on subscriber-settings.

36. The videoconferencing services switch of claim 28, wherein the quality of service module includes a video transmission analysis engine configured to analyze videoconferencing data for quality parameters, based on subscriber-specific transmission analysis settings.

37. The videoconferencing services switch of claim 36, wherein the quality parameters are selected from the group consisting of packet loss, jitter, and latency.

38. The videoconferencing services switch of claim 22, further comprising, a policy engine configured to enforce policies on the videoconferencing call, based on subscriber-specific and/or user-specific settings.

39. The videoconferencing services switch of claim 38, wherein the subscriber-specific and user-specific settings relate to policies selected from the group consisting of outbound/inbound calling privileges, encryption policies, bandwidth policies, priority among users policies, participation privileges, inbound/outbound calling restrictions, time-of-day restrictions, audio restrictions, and video restrictions.

40. The videoconferencing services switch of claim 22, further comprising, a security module having subscriber-specific settings, the security module being configured to prevent unauthorized access to an enterprise subscriber network and to videoconferencing call data.

41. The videoconferencing services switch of claim 40, wherein the security module includes a firewall.

42. The videoconferencing services switch of claim 41, wherein the firewall is configured on a per-subscriber basis, such that a subscriber-specific firewall may be implemented for traffic from each subscriber.

43. The switch of claim 42, wherein the firewall is selected from the group consisting of an SIP firewall and an H.323 firewall.

44. The videoconferencing services switch of claim 40, wherein the security module includes a network address translation (NAT) module configured to provide network address translation services for traffic managed by the call control module.

45. The videoconferencing services switch of claim 44, wherein the network address translation module includes subscriber-specific NAT settings.

46. The videoconferencing services switch of claim 44, wherein the network address translation module is configured to perform address translation selected from the group consisting of SIP network address translation and H.323 network address translation.

47. The videoconferencing services switch of claim 40, wherein the security module includes an encryption module.

48. The videoconferencing services switch of claim 40, wherein the security module includes a virtual private network module configured to create a virtual private network for data streams managed by the call control module.

49. A system for use in videoconferencing, the system comprising:

a service provider network configured to enable users of multiple enterprise subscriber networks to transfer data via a global computer network, the service provider network having an access point; and

a videoconferencing services switch located on the access point of the service provider network, the videoconferencing services switch being configured to process videoconferencing calls from terminals on each of the multiple subscriber networks, based on subscriber-specific settings.

50. The system of claim 48, wherein the switch is configured to provide firewall services for videoconferencing data originating from terminals on each of the multiple subscriber networks, based on subscriber-specific settings.

51. A system for use in videoconferencing, the system comprising:

multiple enterprise subscriber networks, each enterprise subscriber network having one or more videoconferencing terminals;

a service provider network configured to enable users of the multiple enterprise subscriber networks to access a global computer network via an access point; and

a videoconferencing services switch positioned on the access point of the service provider network, the videoconferencing services switch being configured to process videoconferencing calls from terminals of each of the multiple enterprise subscriber networks, based on subscriber specific settings.

52. The system of claim 51, wherein a first enterprise subscriber network includes an enterprise video gateway.

53. The system of claim 52, wherein the enterprise video gateway includes an emulation module configured emulate H.323/SIP call control and firewall functionality.

54. The system of claim 52, wherein the enterprise video gateway include an encryption module configured to encrypt videoconferencing data sent between the videoconferencing services switch and the enterprise video gateway.

55. The system of claim 54, wherein the encryption module is configured to encrypt videoconferencing data using IP Security (IPSec) authentication and encryption.

56. The system of claim 52, wherein the first enterprise subscriber network includes an enterprise router configured to route videoconferencing data to the videoconferencing services switch.

57. The system of claim 52, further comprising, a direct network connection dedicated to video traffic linking the first enterprise subscriber network and the videoconferencing services switch.

58. The system of claim 52, wherein the access point on the service provider network is a point of presence (POP).

59. The system of claim 58, wherein the service provider network includes an edge router configured to route videoconferencing traffic between the multiple subscriber networks and the videoconferencing services switch.

60. The system of claim 58, wherein the service provider network includes a core router configured to route videoconferencing traffic across a computer network backbone to a destination terminal in a remote zone.

61. The system of claim 52, wherein the videoconferencing services switch includes, (1) a virtual router configured to receive a request for a videoconferencing call from an origination terminal via the enterprise gateway, and (2) a call control module configured to perform call set-up operations, manage call data streams, and perform call tear down operations for the videoconferencing call, wherein the virtual router is configured to route call-related traffic between the origination terminal and the call control module.--

In the Abstract:

Please replace the abstract with the following.

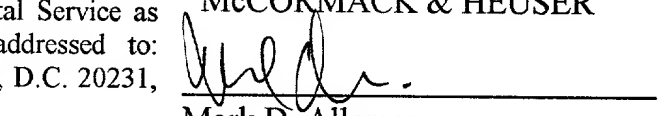
--Abstract

A system, method, and device for use in videoconferencing. The method typically includes installing a videoconferencing services switch at an access point to an IP network, and registering a plurality of subscribers for videoconferencing services. Each subscriber typically has a plurality of endpoints. The method further includes receiving subscriber-specific settings to be applied to multiple videoconferencing calls from the plurality of endpoints associated with each subscriber. The method further

includes storing the subscriber-specific settings at a location accessible to the switch, and configuring the switch to connect calls from the plurality of endpoints at each subscriber based on the corresponding subscriber-specific settings.--

Respectfully submitted,

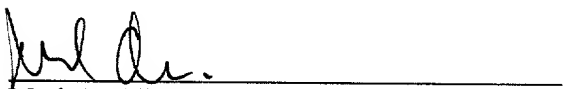
KOLISCH, HARTWELL, DICKINSON, McCORMACK & HEUSER



Mark D. Alleman
Customer No. 23581
Registration No. 42,257
of Attorneys for Applicants
520 S.W. Yamhill Street, Suite 200
Portland, Oregon 97204
Telephone: (503) 224-6655
Facsimile: (503) 295-6679

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner of Patents, Washington, D.C. 20231, on May 18, 2001.



Mark D. Alleman
Date of Signature: May 18, 2001

TO1250 "Express Mail"

VERSION WITH MARKINGS TO SHOW CHANGES MADE

In the Specification:

Please amend paragraph 2 on page 1 as follows.

Technical Field

The present invention relates generally to videoconferencing, and more particularly to a system, method, and device for implementing a[n] multiple subscriber videoconferencing service for use on Internet Protocol (IP) networks.

Please amend paragraph 2 on page 2 as follows.

Videoconferencing over IP networks has a number of fundamental problems, including security, bandwidth utilization, quality of service, and deployment and management. Regarding security, H.323 and SIP are difficult to implement with current firewalls. The difficulty lies in the fact that H.323 and SIP are complex protocols and use multiple dynamically allocated ports for each call. Because of the heavy use of dynamically[-]allocated ports, it is not possible to preconfigure firewalls to allow SIP- or H.323-signaled traffic without opening up large numbers of holes in the firewall. This represents a more lax firewall policy than would be acceptable at most enterprises. In addition, SIP or H.323 video endpoints behind a firewall typically cannot receive calls from external parties due to firewall policies in place at most enterprises.

Please amend paragraph 1 on page 4 as follows.

The above[-]discussed issues lead to another problem with current videoconferencing systems, namely, that enterprises cannot easily outsource videoconferencing services to outside service providers. Currently, service providers are not able to cost-effectively provide videoconferencing services to a large number of subscribers, because specialized equipment must be deployed or existing equipment must be upgraded at every subscriber site. This results in an expensive up-front capital investment as well as significant operational expenses for the service provider. Up-front equipment installations take time at each subscriber, resulting in a slow deployment of the videoconferencing capabilities to subscribers. In addition, the high up-front costs result in decreased service provider profit margins. It is difficult to grow such a service because each subscriber adds to an incremental growth in the capital equipment pool because these resources are not shared.

Please amend paragraph 2 on page 4 as follows.

Because of the cost and reliability issues with ISDN, and because of the security, bandwidth utilization, [and]quality of service, and deployment and management issues with H.323 and SIP, it is difficult for the average enterprise to upgrade and customize its network to enable videoconferencing. In addition, it is difficult for service providers to cost-effectively provide an outsourced videoconferencing service on a per-subscriber basis. Thus there exists a need for a videoconferencing system, method, and

device for delivering secure, high-quality videoconferencing services over an IP network to multiple enterprise subscribers in a manner that does not require expensive upgrading and customization of the enterprise network.

Please amend paragraph 2 on page 5 as follows.

According to another embodiment of the invention, the method may include installing a video services switch on a service provider network at an access point configured to enable multiple enterprise subscribers to access a global packet-switched computer network to exchange data, including videoconferencing data and non-videoconferencing data. The video services switch is typically configured to process videoconferencing data from multiple enterprise subscribers. The method further includes, at the video services switch, receiving a request for a videoconferencing call from an origination endpoint of one of the multiple enterprise subscribers, and connecting the videoconferencing call to a destination endpoint, the videoconferencing call having associated videoconferencing data. The method may further include securing the videoconferencing call based on subscriber-specific security settings.

Please amend paragraph 2 on page 6 as follows.

The system typically includes a service provider network configured to enable users of multiple enterprise subscriber networks to transfer data via a global computer network, the service provider network having an access point. The system also

includes a videoconferencing services switch located on the access point of the service provider network. The videoconferencing services switch [being]is configured to process videoconferencing calls from terminals on each of the multiple subscriber networks, based on subscriber-specific settings.

Please amend paragraph 6 on page 6 as follows.

Fig. 4A is a software architecture of the videoconferencing system of Fig. 1.

Fig. 4B is a continuation of the software architecture of Fig. 4A.

Please amend paragraph 4 on page 7 as follows.

Fig. 9 is a flowchart of one exemplary method for accomplishing the step of configuring the user-specific and subscriber-specific settings of the method of Fig. 6.

Please amend paragraph 3 on page 8 as follows.

Traffic coming into the POP can be classified into videoconferencing data and non-videoconferencing data. Videoconferencing data typically includes control data and streaming voice and audio data according to the H.323 or SIP standards. H.323 refers to International Telecommunications Union, Telecommunications Sector, Recommendation H.323 (version 1, published November 1996;[,] version 2, published 1998, entitled, "Visual Telephone Systems and Equipment for Local Area Networks Which Provide a Non-guaranteed Quality of Service," the disclosures of which are herein

incorporated herein by reference. SIP refers to Session Initiation Protocol Proposed Standard (RFC 2543), Internet Engineering Task Force (IETF) (published March 1999), the disclosure of which is incorporated herein by reference. Non-videoconferencing data includes, for example, email, web pages, VOIP traffic, VPN traffic, etc. Videoconferencing data is typically routed through POP 16 via videoconferencing services switch 12, while non-videoconferencing data is routed around the switch.

Please amend paragraph 2 on page 9 as follows.

Each of enterprise subscriber networks 18 typically includes a plurality of terminals 34. Terminals 34, along with video conferencing service switch 12 and the various other components of system 10, are typically H.323 or SIP compliant. Terminals 34 are typically videoconferencing devices configured to display and record both video and audio. Terminals 34 may be desktop computers, laptop computers, mainframes and/or workstation computers, or other videoconferencing devices. Terminals 34 may also be described as "endpoints" in a videoconferencing call. The terminal 34a originating the videoconferencing call is referred to as an origination endpoint 34a, and the other terminals requested to join in the call are referred to as destination terminals, shown at 34b, 134a, 134b. Terminal 34b is a local zone destination terminal, while terminals 134a, 134b are remote zone destination terminals. Local and remote zones are defined below.

Please amend paragraph 4 on pages 9-10 as follows.

Enterprise video gateway 36 typically includes an emulation module 40 which emulates H.323/SIP call control and firewall functionality and an encryption module 44. The gateway also typically has a globally routable IP address and is configured to manage secure communication between terminals 34 and the videoconferencing services switch 12. Typically, emulation[firewall] module 40 appears to terminals 34 as H.323 gatekeeper/SIP proxy and H.323/SIP application proxy firewall which includes network address translation (NAT) capability, which hides internal address from outside devices.

Please amend paragraph 2 on page 10 as follows.

As shown in Fig. 10, enterprise video gateway 36 includes an encryption module 44. Encryption module 44 is typically an IP Security (IPSec) authentication and encryption module 44 configured to encrypt videoconferencing data coming from terminals 34 and send the encrypted data to videoconferencing switch 12. The IPSec protocols [are]have been adopted by the Internet Engineering Task Force, and are described in the RFC 2411 entitled "IP Security Document Roadmap" (published Nov. 1998), the disclosure of which is herein incorporated by reference. By using IPSec, a Virtual Private Network (VPN) may be created between the gateway 36 and the switch 12. VPN refers to a network that is carried over public networks, but which is encrypted to make it secure from outside access and interference.

Please amend paragraph 3 on page 11 as follows.

System 10 may be configured to connect a two-party or multiparty videoconference call from an origination terminal 34a to a destination terminal 34b on local zone 11, and/or one or more destination terminals 134a and 134b on remote zone 111. A destination terminal on local zone 11 may be referred to as a local destination terminal, and a destination terminal on remote zone 111 may be referred to as a remote destination terminal.

Please amend paragraph 5 on pages 11-12 as follows.

Each enterprise subscriber network 218 includes a plurality of terminals 234 which are similar to terminals 34 described above. Integrated Access Device (IAD) 246 is configured to receive traffic from enterprise subscriber networks 218 and forward the traffic to the Digital Subscriber Line Access Multiplexor (DSLAM) 248. The DSLAM is configured to multiplex the traffic from the IADs and forward it to Asynchronous Transmission Mode (ATM) switch 250, where the signals are demultiplexed for transmission over a long-haul backbone. ATM switch 250 is configured to route videoconferencing data to and from terminals 234 and the backbone via videoconferencing services switch 212, and non-videoconferencing data via ISP router 252, or another services switch.

Please amend paragraph 2 on page 12 as follows.

Fig. 3 shows an exemplary hardware configuration for videoconferencing services switch 12. One switch that may be purchased and programmed to implement the present invention is the Intel Exchange Architecture (IXA) WAN/Access switch, commercially available from Intel Corporation, of Santa Clara, California and Radisys Corporation of Hillsboro, Oregon.

Please amend paragraph 3 on pages 12-13 as follows.

Switch 12 typically includes a control plane module 302 and a data plane module 304. Control plane module 302 includes a host processor, linked to an input/output network interface 308 and a memory 310. Typically, memory 310 includes RAM and ROM, although another form of memory may also be used, such as flash memory. Alternatively, a storage device such as a hard drive may also be attached to host processor 306. Control plane module 302 is configured to receive control data such as call set-up information through network interface 308, data plane ingress port 318, or data plane egress port 320. The call set-up information is processed according to H.323 or SIP specifications by host processor 306. Typically, the programs and data necessary for processing the call are stored in memory 310 and implemented by host processor 306. For example, the virtual router, call control module, quality of service module, policy engine, and security module are typically stored in memory 310.

Please amend paragraph 2 on page 13 as follows.

Control plane module 302 is linked to data plane module 304 via a bus 312. Data plane module 304 includes a network processor 314 and memory configured to receive and manage transfer of real-time audio and video data streams from ingress ports 318 to egress ports 320. Data plane module 304 typically includes a wire-speed switching fabric, capable of processing real-time data streams with virtually no appreciable latency.

Please amend paragraph 3 on page 13 as follows.

The wire-speed switching fabric is configured to enable transport of streaming data traffic across system with virtually no appreciable latency, even as the streaming data traffic is processed and analyzed by system 10 to impose H.323/NAT-specific firewall and NAT capabilities, policies from policy engine 418, monitor quality of service, and provide optional encryption and other security measures. One implementation of system 10 is configured to provide aggregate streaming data throughput[throughout] of up to 1.048 Gbps with full security and policy management, quality of service management, and encryption. The wire-speed switching fabric includes full support for IETF standard IP routing protocols such as Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), and Routing Information Protocol (RIP), which are well known in the networking arts. Support of these routing protocols will allow system 10 to forward video traffic appropriately to edge router 20 and core router 22 in the service provider access point 116.

Please amend paragraph 2 on page 14 as follows.

Terminal settings 408a typically include the IP address of the enterprise gateway, which acts as a proxy to the call control module 413 in videoconferencing switch 12. For calls placed with the H.323 protocol, the IP address of the enterprise gateway 36 (which also acts as a proxy to the videoconferencing services switch H.323 gatekeeper 414) is provided. For calls placed with the SIP protocol, the IP address of the enterprise gateway 36 (which also acts as a [the]proxy to the videoconferencing services switch SIP proxy 416) is provided. Terminals use the IP address of the enterprise gateway for registration (using e.g. H.323 RAS signaling), call initiation (using e.g. H.323 ARQ signaling), and audio/video data exchange (using e.g. RTP/RTCP protocols). Users may optionally authenticate themselves with H.323 gatekeeper/SIP proxy. The enterprise gateway 36 encapsulates these messages in packets having the enterprise video gateway's globally routable IP address as the source address and forwards these messages to the call control module 413 in videoconferencing services switch 12. Typically, these packets are sent in an encrypted form using IPSec.

Please amend paragraph 2 on page 15 as follows.

Enterprise edge router settings 408b typically include the globally routable IP address of the enterprise gateway 36, and the address of an H.323 gatekeeper 414 and/or SIP proxy 416 within the videoconferencing services switch 12. The enterprise edge router may also be configured to direct traffic from a terminal to the gatekeeper 414

or proxy 416 along direct connection 42. Enterprise edge router settings 408b may also include prioritization information for traffic passing though the edge router, such that the router may tag packets passing through with Diff-Serv labels or process packets based on Diff-Serv labels.

Please amend paragraph 3 on page 16 as follows.

Calls in the H.323 protocol are routed to virtual H.323 gatekeeper 414, while calls in the SIP protocol are routed to SIP Proxy 416. Call control module 413 is configured to perform call set-up operations, manage call data streams, and perform call tear-down operations.

Please amend paragraph 3 on page 18 as follows.

Quality of service module 420 also includes an IP-over-ATM module 428 configured to send IP traffic over ATM switches, and settings 408k therefor. IP over ATM module is compliant with the standards described in Internet Engineering Task Force Request for Comments (RFC) 2684. Typically, settings 408k for IP-over-ATM module 428 are configured on a per-virtual router and per-physical interface basis.

Please amend paragraph 5 on pages 18-19 as follows.

Videoconferencing services switch 12 also typically includes a security module 431. Security module 431 typically includes a SIP/H.323 firewall 432, SIP/H.323

NAT module 434, encryption module 436, and Virtual Private Network (VPN) module 438. SIP/H.323 firewall 432 is configured to prevent unauthorized access to video services switch 402, and through it to subscriber networks. The firewall settings 408n of firewall 432 are configured on a per-subscriber basis, such that a subscriber-specific firewall may be custom-implemented for traffic from each subscriber. SIP/H.323 NAT module 434 is configured to provide network address translation services for traffic flowing through switch 12. NAT settings 408l are also subscriber-specific. VPN module 438 is configured to create a virtual private network for data flowing from switch 12 over network 20.

Please amend paragraph 3 on pages 19-20 as follows.

Videoconferencing services management application 402 is configured to interface with a database 404, which contains a database image 406 of records for subscriber-specific settings 408 for each of the multiple enterprise subscriber networks 18. Many of the subscriber-specific settings 408 are governed by a Service Level Agreement (SLA) 409. The SLA is an agreement executed between each enterprise subscriber and the service provider. The SLA contains terms for the level of videoconferencing service to be provided to a particular enterprise subscriber network. One exemplary term contained in the SLA is a video quality term, which indicates the maximum and/or minimum video quality the subscriber is to receive, either on a per-subscriber, per-user, or per-terminal basis. Often, video quality is defined as packet loss,

jitter, and latency being within an acceptable predetermined range. While, typically, terminal settings 408a and enterprise router settings 408b are stored locally on enterprise subscriber network 18, it will also be appreciated that they may be stored on database 404. The switch resident settings are typically loaded into video services switch 12 periodically, such as once per day, by downloading database image 404 into memory of switch 12. The enterprise video gateway server settings 408r may be downloaded in a similar manner from database 404 via videoconferencing services management application 402.

Please amend paragraph 2 on page 23 as follows.

Step 510 includes, at 612, configuring a call-control module. At 614, step 612 includes configuring H.323 gatekeeper 414 and/or SIP proxy 416 for subscriber 18. For H.323 gatekeeper 414, configuring gatekeeper 414 includes configuring a subscriber zone in gatekeeper 414, discovery and registration of endpoints, security, inter-gatekeeper communication, creation of records for billing and administrative purposes, etc. For SIP proxy 416, configuring proxy 416 includes discovery and registration of endpoints, information from Domain Name Service (DNS) server, creation of records, etc.

Please amend paragraph 2 on page 24 as follows.

Step 616 further includes configuring the encryption module at 706. Encryption is [only]used only at certain enterprise subscribers 18 and destination IP

addresses. For example, enterprises 18 may want encrypted communication with selected destination parties.

Please amend paragraph 3 on page 24 as follows.

Lastly, step 616 includes configuring virtual private network (VPN) module at 708. Configuring VPN module includes configuring a subscriber VR with MPLS VPN capability including creation of VPN routing/forwarding tables. Step 708 further includes configuring BGP routing sessions, VR to SP edge-routing sessions, RIP/BGP/static route to subscriber edge-routing sessions, etc. By configuring switch 12 to support an MPLS VPN module, video-specific VPNs can exist across ATM, IP and L2-type backbone networks. In addition, subscribers to MPLS VPNs may be dynamically updated to enable simplified creation of extranet and intranet VPNs and site-to-site video traffic delivery.

Please amend paragraph 3 on page 25 as follows.

At 806, the method further includes configuring differentiated services (Diff-Serv) module 426 at 806, typically by adjusting Diff Serv settings 408j. These settings may be used to configure the TOS/IP precedence field for video traffic (i.e. RTP streams) to/from each enterprise. This enables core devices in an SP network to give prioritized treatment to video traffic.

Please amend paragraph 5 on page 25 as follows.

At 810, the method further includes configuring video transmission analysis module[at 810], typically by adjusting settings 408m. Configuration of size of jitter buffer within the videoconferencing services switch is accomplished on a per-enterprise subscriber basis.

Please amend paragraph 6 on pages 25-26 as follows.

Fig. 9 shows, in steps 902-918, one exemplary method of accomplishing step 620 of configuring user-specific and subscriber-specific policies on policy engine 418. The method typically includes, at 902, setting access privileges. Access privileges govern who can access the video system with user level and administrator level access privileges. At 904, the method includes setting inbound/outbound calling privileges on a per-user or per-subscriber basis. For example, every user in an enterprise may be prohibited from making outbound calls on company holidays, except upper management. At 906, the method typically includes setting time-of-day privileges per user or subscriber. For example, every user may be restricted from placing calls outside of regular business hours. At 908, the method typically includes setting maximum video quality privileges per user, or per subscriber.

Please amend paragraph 2 on page 26 as follows.

At 910, the method typically includes setting 2-way support privileges. This allows a user to either send, receive, or both send and receive videoconferencing data

pertaining to a call. At 912, the method includes setting audio-only restrictions on a per-user or per-subscriber basis. The method includes [At]setting encryption requirements at 914. At 916, the method typically includes setting priority privileges on a per-user or per-subscriber basis. Videoconferencing data sent by a user with higher priority privilege will take precedence over other data sent by a user of lower priority, or over other lower priority data, such as email. At 918, the method typically includes setting videoconferencing call screening. This enables a user or subscriber to block incoming calls from a user-specified source. The policies set in step 620, and substeps 902-918 are typically saved as user-specific and subscriber-wide settings 408f, 408g.

In the Claims:

Please amend claims 1, 5-8, and 10, as follows.

1. (Amended) A method for videoconferencing using Internet Protocol (IP), the method comprising the steps of:

installing a videoconferencing services switch at an access point to [an] a service provider IP network;

at the switch, registering a plurality of subscribers for videoconferencing services, each subscriber including a plurality of endpoints;

receiving subscriber-specific settings to be applied to multiple videoconferencing calls from the plurality of endpoints associated with each subscriber;

storing the subscriber-specific settings at a location accessible to the switch;

and

configuring the switch to connect calls from the plurality of endpoints at each subscriber based on the corresponding subscriber-specific settings.

5. (Amended) A method for use in videoconferencing, the method comprising:

installing a videoconferencing services switch on a service provider network at an access point configured to enable multiple enterprise subscribers to access a global packet-switched computer network to exchange data, including videoconferencing data and non-videoconferencing data, the videoconferencing services switch being configured to process videoconferencing data from multiple enterprise subscribers;

at the videoconferencing services switch, receiving a request for a videoconferencing call from an origination endpoint of one of the multiple enterprise subscribers;

connecting the videoconferencing call to a destination endpoint, the videoconferencing call having associated videoconferencing data; and

securing the videoconferencing call based on subscriber-specific security settings.

6. (Amended) The method of claim 5, wherein each enterprise

subscriber includes an enterprise gateway positioned on the network between the access point and the origination endpoint, the method further comprising:

routing videoconferencing data from the enterprise gateway to videoconferencing services switch; and

routing non-videoconferencing data from the enterprise gateway around the videoconferencing services switch.

7. (Amended) The method of claim 6, wherein the videoconferencing data is routed to the videoconferencing services switch via a direct network connection from an enterprise router to the videoconferencing services switch.

8. (Amended) The method of claim 6, wherein the video[ ]conferencing data is routed to the videoconferencing services service switch through an access point edge router.

10. (Amended) The method of claim 9, wherein the video[ ]conferencing data routed through the firewall is encrypted.

New claims 21-61 are also added, as detailed above.

In the Abstract:

Please amend the abstract as follows.

Abstract

A system, method, and device for use in videoconferencing. The method typically includes installing a videoconferencing services switch at an access point to an IP network, and registering a plurality of subscribers for videoconferencing services. Each subscriber typically has a plurality of endpoints. The method further includes receiving subscriber-specific settings to be applied to multiple videoconferencing calls from the plurality of endpoints associated with each subscriber. The method further includes storing the subscriber-specific settings at a location accessible to the switch, and configuring the switch to connect calls from the plurality of endpoints at each subscriber based on the corresponding subscriber-specific settings.